

Remarks :**Claim 10 as amended contains no new matter and raises no new issue**

In claim 10 as amended, "computer readable medium being in form of data signal embodied in a carrier wave" is not new matter. Note that the "computer code" of claim 22, upon which claim 10 as amended depends, is being stored in the medium and corresponds to "the central program" of the description and as readable on sheet 7, last paragraph, lines 1,2, "the central program is being installed in a harddisk of a user computer", this implicitly indicates the central program which may be obtained from a disk or internet, is being transferred to the harddisk in the form of data signal embodied in a carrier wave.

Claim 10 as amended raises no new issue as it is readable on claim 9 (withdrawn).

Patentability of Independent Claims 1, 14, 18, 20, 21 as amended**Examiner's rejection :**

As the Examiner has admitted in the Final Office action, P.6, section 13, second paragraph, in his arguments in support of 103 rejection of claims 1, 2, 4, 14, 15 and 17-22, "The Wiedemer patent provides for an identity means to determine authorization if a user and provides for information that leads to a billing charge, but does not disclose the step of not causing ..electronic commerce operation to be performed".

But the Examiner further stated, in the Final Office action, P.6, section 13, third paragraph, "The patent to Haas et al teaches a method for providing secure access to shared information such as a newspaper, see column 1, lines 20-35. The Haas patent teaches deterrents for discouraging users from providing useful information to others to access the information in question. Column 5, lines 47-54 teach a first deterrent as causing a rightful user's credit card number to display to discourage a rightful user from sharing the information to access the secured information to others".

The Examiner concluded in the fourth paragraph, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wiedemer method as taught in Hass by causing a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others who are not the rightful user(s).

Applicant's reasons :

The Examiner's rejection is respectfully traversed, for the following reasons :

The Examiner incorrectly applies Haas et al's deterrent to Wiedemer, for the following reasons:

- 1) It is respectfully submitted that, Wiedemer's billing system's most important purpose is to monitor usage of a software so as to charge a user based on amount of usage of the same software (refer to abstract), therefore if its purpose is to be changed to charge the user in the form of regular subscription (refer to Haas et al, col., 2, lines 8,9, "suitable for use in providing secure access electronic newspapers and multimedia documents"; col., 3, lines 56-59, "the user i transmits ...his credit card number (for billing purposes)"; col. 4, lines 45, 46, "a user's access permission expires") or a fixed price for perpetual use(as mentioned in Wiedemer, "Background of the invention", col. 1, lines 19-23) or the like, etc., such that payment is independent of amount of usage, then there would require a substantial reconstruction and redesign of the elements in Wiedemer's billing system as well as a change in the basic principle under which the construction was designed to operate. Therefore, it would not be obvious to one with ordinary skill in the art to modify Wiedemer's billing system to not do the monitor work during the time the protected software is being used and not to charge a user based on amount of usage, so as to meet the important limitation of claim 1 as amended that "use of said software is being permitted without causing said account being accessed".
- 2) Wiedemer's requirement of "monitoring usage of software so as to charge a rightful user based on amount of usage of software", that is billing operation,

is already providing a better effect of discouraging the rightful user from sharing a software with other people, than Haas et al's deterrent. Because if the rightful user allows another person to use the software, he is bound to be charged by Wiedemer's billing system, whereas Haas et al's deterrent although will display the rightful user's credit card information to that person, that person may not make use of the information to make any transaction. Thus, there has no motivation for one with ordinary skill in the art to modify Wiedemer's billing system with Haas et al's deterrent.

- 3) Further, the purpose of Wiedemer's billing operation is to charge a rightful user basing on the amount of usage, and to make money. Therefore, as long as the usage of software can be monitored and the rightful user can be charged, then one with ordinary skill in the art would not prevent other person from using the protected software under the permission of the rightful user, by applying Haas et al's deterrent to Wiedemer. In doing so, the prime purpose of Wiedemer, that is, making money, will be undermined.

If Wiedemer method was to be modified with Haas et al's deterrent, the result would be a method comprising 1) Wiedemer's billing system to monitor usage of software so as to charge a user based on amount of usage of software; as well as 2) Haas et al's deterrent which causes a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others.

Thus, in the combination, the above Examiner's reasons for Wiedemer alone cannot meet claim 1 as amended is also applicable to the result as far as the part corresponding to Wiedemer's billing system therein is concerned. Similarly, the reasons for Haas et al. failing to meet claim 1 as amended is also applicable to the result as far as the part corresponding to Haas et al's deterrent therein is concerned, as

follows :

The present invention as claimed by claim 1 as amended is directed to a method for protecting software from unauthorised use.

As readable thereon, it requires "determining if identity information is existing in a personal processing apparatus storing said software"; and "using said identity information being determined as existing as a pre-condition for causing said personal processing apparatus to permit user to use said software"

Further, the "identity information being used on the personal processing apparatus for generating another information for to be authenticated by a remote computer, so as to access a financial account of a rightful user of the software"; and

"use of said software is being permitted without causing said account being accessed and without having information capable of being used for accessing a user financial account be provided in a user accessible and human-recognizable form" and the "identity information being specific to the rightful user".

As seen, claim 1 as amended is directed to a method useful for protecting a software from unauthorised use at a time no payment for the use thereof is required, for reason such as payment is being made at a earlier time.

Even though Haas et al's deterrent can meet the amended claim 1's requirement of "use of said software is being permitted without causing the account being accessed", it fail to meet a newly added requirement "use of said software is being permitted.... without having information capable of being used for accessing a user financial account be provided in a user-accessible and human-recognizable form".

It is an essential feature in Haas et al.'s deterrent that a rightful user's credit card number has to be displayed, this has a drawback that the rightful user have to

make sure no other people is around before he can use the software. And, it would not be obvious to one with ordinary skill in the art to modify it by not having the credit card number to be displayed; and further to make use of the electronic transaction capability of the credit card number to create "identity information" for providing another information...to access a financial account" of claim 1 as amended and meeting the newly added requirement such that it is not "in a user-accessible and human-recognizable form"; and still further, using the identity information being determined as existing as a pre-condition for causing the personal processing apparatus to permit user to use the software", but "without causing the account being accessed", so as to amount to the present invention as defined by claim 1 as amended.

Accordingly, 103(a) rejection of claim 1 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Regarding claim 14 as amended, it is equivalent to claim 1 as amended in that it contains all requirements of claim 1 as amended and its requirement of "authenticating an identity information" implicitly requires "determining existence of the identity information" as claim 1 as amended does.

Therefore, if claim 1 as amended is allowable, then claim 14 as amended should be allowable as well. Accordingly, 103(a) rejection of claim 14 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Regarding claim 18 as amended, it recites a method comprising a sub-method for "using a favourable result of a verification of validity of a user's account as a pre-condition for permitting use of the protected software on a processing apparatus", at a cost. Thereafter, the sub-method capable of being used for permitting use of software on a second processing device, without re-charging the

cost.

Thus, a user who has paid for the protected software, can use the same on any processing device he desires or on the original processing device after changes in software/hardware, without being fully re-charged, by the present method as defined by claim 18 which assures the software vendor that the protected software will continue to be used by that user.

The requirement of claim 18 as amended that "verification of validity of a user's account as a pre-condition for permitting use of the protected software on a second processing apparatus, without re-charging the cost of the software" is neither disclosed or suggested by Haas et al and Wiedemer, considered individually or in combination.

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claim 18 and its dependent claims 19 are respectfully requested.

Regarding independent claim 20 as amended, it recites a method comprising a sub-method which after recognizing (refer to step (a)) a first processing apparatus meeting an "Installation" pre-condition, will thereafter permit software to be used on the recognized processing apparatus, without the "installation" pre-condition being met. Further, the sub-method is capable of being used for recognising another processing apparatus also meeting the "installation" pre-condition, without a step relating to a new user payment therefor.

The "installation" pre-condition requires "identity information/means being specific to said user and capable of being used on said personal processing apparatus for generating another information for to be authenticated by a remote computer, so as to access a financial account of a rightful user of said software", presents in a

processing apparatus.

It should be noted that the phrase "capable of being used" implies that if the "identity information/means" is password protected or the like, then the protection have to be removed by entry of user password in order to meet the "installation" pre-condition. This is readable on the original filed specification P.7, last paragraph-P.9, second paragraph. Particularly, in P.7, last paragraph lines 1,2, it is readable thereon that "when the central program is being installed in a harddisk of a user computer and executed"—the execution of the central program, and further execution of the EI sub-program(P.5,section 2) therein which corresponds to "identity software/means" of claim 20 as amended, requires entry of user password, for details pls refer to P.4, section 1a.

The present invention not being suggested or disclosed by the cited prior art references Haas et al and the 2 Wiedemer patents, either considered individually or in combination.

Claim 20 as amended recites "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform ... step (a)". This actually means that the protection software either determines the presence of identity information/means, like claim 1 as amended, or being combined with the identity program code in a non-separable manner, like claim 7 as amended.

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claim 20 is respectfully requested.

Regarding independent claim 21 as amended, although not readable on claim 21 as amended, the present invention as defined by claim 21 as amended is

directed to a method for protecting a data processing apparatus from unauthorised use.

It is respectfully submitted that, it is an innovative feature of the present invention as defined by independent claim 21 as amended that , verifying identity of a user of a data processing apparatus, a) by receiving information specific to a user and necessary for accessing an account of the user; b) verifying the user account being valid; c) and using a favourable result of the verification as a pre-condition for providing user access to at least a part of the functionality of the data processing apparatus, without charging the account and that at least a part of functionality being not related to the validity status of the account.

Throughout Haas et al and Wiedemer, whole document, there is no disclosure or suggestion that "validity of a user account should be checked, without charging the account for providing the user access to a data processing apparatus", as required by claim 21. In Haas et al. at column 3 lines 55-60, "the user i transmits ...his credit card number (for billing purposes)", it is clear that the credit number which is for billing purposes cannot meet this important requirement of claim 21 as amended .

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claim 21 is respectfully requested.

Patentability of Independent Claim 7 as amended**Examiner's rejection :**

The Examiner states in the Final Office Action, P.5, section 12, that "SECURITY MODULE 16 corresponds to the recited identity software. Column 6 lines 41-49 describes that the billing module provides information for enabling a billing operation to the user take place whenever the protected software is to be executed".

Applicant's reasons :

Claim 7 as amended now recites the "authorising software. ..for...permitting user to use said software, without causing any user financial account being charged", this clearly means no billing operation is necessary.

The present invention as defined by claim 7 allow unrestricted rightful use of protected software while offering protection against unauthorised use by requiring the authorising software be contained in the protection software product with the identity program code, and can not be copied therefrom individually. The identity program code being for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible.

Accordingly, Wiedemer(4,796,181) cannot meet independent claim 7 and the rejection thereof and its dependent claims 8, 9 should be withdrawn .

In additional, another reference Haas et al is also considered, and it cannot meet claim 7 as amended, either considered individually or in combination with Wiedemer(4,796,181). For details, pls refer to P.21, the paragraph begin with "If Wiedemer method was to be modified with Haas et al's deterrent".

Haas et al.'s deterrent suggest that a rightful user's credit card number has to be

displayed, this is in contrast with claim 7 as amended's requirement of "authorising software... for...permitting user to use said software,... without having information capable of being used for accessing a user financial account be provided in a user-accessible and human-recognizable form".

Patentability of Independent Claims 12, 16 as amended**Examiner's rejection :**

As the Examiner has admitted in the Final Office action, P.7 section 14, second paragraph, in his arguments in support of 103 rejection of claims 12, 13, 16 , "The Second Wiedemer patent (5,155,680) discloses a billing system similar to the first Wiedemer patent (4,796,181) and provides the same component...this patent also provides for PIN, i.e. password protection".

The Examiner further stated, in the Final Office action, P.7, section 14, third paragraph, "Haas et al teaches a method for providing secure access to shared information such as a newspaper, see column 1, lines 20-35. The Haas patent teaches deterrents for discouraging users from providing useful information to others to access the information in question. Column 5, lines 47-54 teach a first deterrent as causing a rightful user's credit card number to display to discourage a rightful user from sharing the information to access the secured information to others".

Finally the Examiner concluded in the fourth paragraph, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wiedemer method as taught in Hass by causing a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others who are not the rightful user(s).

Applicant's reasons :

Regarding claim 12 as amended, it is equivalent to claim 1 as amended in that it contains all requirements of claim 1 as amended and its requirements of "a processing apparatus storing identity information" and "obtaining correct first information (equivalent to password or the like for the identity information) from a

user as a pre-condition for causing said personal processing apparatus to permit user to use said software" is equivalent to steps of "determining" and "using" of claim 1 as amended.

Therefore, if claim 1 as amended is allowable, then claim 12 as amended should be allowable as well. Accordingly, 103(a) rejection of claim 12 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

Regarding independent claim 16 as amended, it recites a method in which if first information is obtained from a user in step (a), then in step (b), it will determine second information related to the hardware or/and software of a processing apparatus, and thereafter, in steps (c) & (d), using a processing apparatus being authentic as a precondition for permitting use of software desired to be protected thereon, without re-obtaining the first information from a user.

Claim 16 as amended also recites the first information has to be consistent with third information which being confidential information of a rightful user of said software desire to be protected and being necessary for accessing a financial account of a rightful user of the software; and the method is being performed without causing said account being accessed, this implicitly indicates no charge to the account.

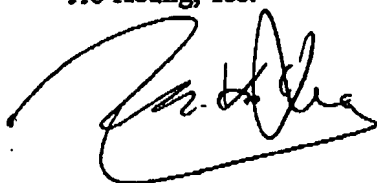
In conclusion, claim 16 as amended is directed to a method for protecting software from unauthorized use, basing on hardware or/and software configuration/characteristics of a processing apparatus of a user, but at the same time enables the user to use the protected software on different processing apparatus with different software/hardware characteristics, without recharging the user once the cost of the protected software has been paid, and without re-entering the confidential first information. This is an innovative feature of the present invention not being suggested

or disclosed by the cited prior art references Haas et al and the 2 Wiedemer patents,
either considered individually or in combination.

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent
claim 16 is respectfully requested.

Respectfully submitted,

Ho Keung, Tse.

A handwritten signature in black ink, appearing to read 'Ho Keung, Tse.', written over a horizontal line.